

PART 2700—SECURITY INFORMATION REGULATIONS

Subpart A—Introduction

Sec.

- 2700.1 References.
- 2700.2 Purpose.
- 2700.3 Applicability.

Subpart B—Original Classification

- 2700.11 Basic policy.
- 2700.12 Criteria for and level of original classification.
- 2700.13 Duration of original classification.
- 2700.14 Challenges to classification.

Subpart C—Derivative Classification

- 2700.21 Definition and application.
- 2700.22 Classification guides.

Subpart D—Declassification and Downgrading

- 2700.31 Declassification authority.
- 2700.32 Declassification general.
- 2700.33 Mandatory review for declassification.
- 2700.34 Downgrading authority.

Subpart E—Safeguarding

- 2700.41 General restrictions on access.
- 2700.42 Responsibility for safeguarding classified information.
- 2700.43 Reproduction controls.
- 2700.44 Administrative sanctions.

Subpart F—Implementation and Review

- 2700.51 Information Security Oversight Committee.
- 2700.52 Classified Review Committee.

AUTHORITY: E.O. 12065, National Security Regulation of June 28, 1978 (43 FR 28949, July 31, 1978); Information Security Oversight Office Directive No. 1 (43 FR 46280, October 5, 1978).

SOURCE: 44 FR 51574, Sept. 4, 1979, unless otherwise noted. Correctly designated at 44 FR 51990, Sept. 6, 1979.

Subpart A—Introduction

§ 2700.1 References.

(a) Executive Order 12065, “National Security Information,” June 28, 1978, (hereinafter E.O. 12065).

(b) Information Security Oversight Office, Directive No. 1, “National Security Information,” October 2, 1978, (hereinafter ISOO Directive No. 1).

§ 2700.2 Purpose.

The purpose of this Regulation is to ensure, consistent with the authorities listed in § 2700.1, that national security information originated and/or held by the Office for Micronesian Status Negotiations (OMSN), which includes the Status Liaison Office, Saipan, Northern Mariana Islands (SLNO), is protected. To ensure that such information is protected, but only to the extent and for such period as is necessary, this regulation identifies the information to be protected and prescribes certain classification, declassification and safeguarding procedures to be followed.

§ 2700.3 Applicability.

This Regulation supplements E.O. 12065 within OMSN with regard to National Security Information. In consonance with the authorities listed in § 2700.1, it establishes general policies and certain procedures for the classification, declassification and safeguarding of information which is owned by, is produced for or by, or is under the control of OMSN.

Subpart B—Original Classification

§ 2700.11 Basic policy.

(a) *General.* It is the policy of OMSN to make available to the public as much information concerning its activities as is possible, consistent with its responsibility to protect the national security.

(b) *Safeguarding national security information.* Within the Federal Government there is some information which because it bears directly on the effectiveness of our national defense and the conduct of our foreign relations, must be subject to some constraints for the security of our nation.

(c) *Balancing test.* To balance the public's interest in access to government information with the need to protect certain national security information from disclosure, these regulations identify the information to be protected, prescribe classification, downgrading, declassification, and safeguarding procedures to be followed, and establish education, monitoring and

§ 2700.12

sanctioning systems to insure their effectiveness. When questions arise as whether the need to protect information may be outweighed by the public interest in disclosure of the information, they shall be referred to OMSN pursuant to § 2700.32(b) for a determination whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.

§ 2700.12 Criteria for and level of original classification.

(a) *General Policy.* Documents or other material are to be classified only when protecting the national security requires that the information they contain be withheld from public disclosure. Information may not be classified to conceal violations of law, inefficiency, or administrative error, or to prevent embarrassment to a person, organization or agency, or to restrain competition. No material may be classified to limit dissemination, or to prevent or delay public release, unless its classification is consistent with E.O. 12065.

(b) *Criteria.* To be eligible for classification, information must meet two requirements:

(1) First, it must deal with one of the criteria set forth in section 1-301 of E.O. 12065;

(2) Second, the President's Personal Representative for Micronesian Status Negotiations or his delegate who has original classification authority must determine that unauthorized disclosure of the information or material can reasonably be expected to cause at least identifiable harm to the national security.

(c) *Classification designations.* Only three designations of classification are authorized—"Top Secret," "Secret," "Confidential." No other classification designation is authorized or shall have force.

(d) Unnecessary classification, and classification at a level higher than is necessary, shall be avoided. If there is reasonable doubt as to which designation in section 1-1 of E.O. 12065 is appropriate, or whether information should be classified at all, the less restrictive designation should be used, or

32 CFR Ch. XXVII (7-1-12 Edition)

the information should not be classified.

§ 2700.13 Duration of original classification.

(a) Information or material which is classified after December 1, 1978, shall be marked at the time of classification with the date or event for declassification or a date for review for declassification. This date or event shall be as early as national security permits and shall be no more than six years after original classification except as provided in paragraph (b) of this section.

(b) Only the President's Personal Representative for Micronesian Status Negotiations may authorize a classification period exceeding six years. Originally classified information that is so designated shall be identified with the authority and reason for extension. This authority shall be used sparingly. In those cases where extension of classification is warranted, a declassification date or event, or a date for review shall be set. This date or event shall be early as national security permits and shall be no more than twenty years after original classification except that for foreign information the date or event may be up to thirty years after original classification.

§ 2700.14 Challenges to classification.

If holders of classified information believe the information is improperly or unnecessarily classified, or that original classification has been extended for too long a period, they should discuss the matter with their immediate superiors or the classifier of the information. If these discussions do not satisfy the concerns of the challenger, the matter should be brought to the attention of the chairman of the OMSN Information Security Oversight Committee, established pursuant to § 2700.51. Action on such challenges shall be taken within 30 days from date of receipt and the challenger shall be notified of the results. When requested, anonymity of the challenger shall be preserved.